

***The summary of a doctoral dissertation by Marcin Rojszczak entitled  
"Protection of privacy in cyberspace in Polish and international law, taking into account  
threats resulting from new information processing technologies"***

The subject of the thesis is an attempt to assess whether existing or planned laws are an effective means of protecting privacy against threats related to new information processing technologies. In recent years, the problem of the maladjustment of legal norms to the regulation of events taking place in cyberspace has been more and more often indicated as one of the barriers to further evolution towards a knowledge-based society. Modern processing techniques, such as cloud computing, big data analytics and the Internet of Things entail not only new possibilities, but also as yet unknown threats, including those to the fundamental rights.

In the analysis of the above problem, particular attention was paid to the discussion of supranational regulations related to both human rights systems and data protection laws. For over fifty years human rights systems have constituted a legally binding international mechanism for the protection of the fundamental rights, including the right to privacy. The work discusses and analyses the content of this right and the scope of protection stipulated, inter alia, by the provisions of the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

The EU law system was also analyzed in detail, including the reformed European data protection model based on the provisions of Regulation 2016/679. The example of EU law was used to seek an answer to the question of whether transnational EU law has the potential to standardize privacy protection, and thus to create a secure data processing space that goes beyond the borders of the EU Member States.

It was also considered whether and to what extent the national legislature may, through local regulations, fill gaps or deficiencies related to the functioning of supranational regulations. In a broader perspective, is it possible to ensure the protection of privacy in cyberspace through norms whose scope of application is determined by the borders of particular states?

The main goal of the presented considerations was to examine the imperfections of the applicable legal norms at the national, EU and international levels. At the same time, based on partial results, it became possible to formulate *de lege ferenda* conclusions regarding the key

factors that should be taken into account in the future legislation, so that the law enacted can solve the identified problems in an appropriate manner.

The dissertation is divided into eight chapters, grouped in two parts. The first chapter discusses key terms such as *privacy*, the related *right to privacy*, as well as *cyberspace* and the relationship between data protection and privacy. The second chapter presents an analysis and discussion of the most important human rights systems which function in the Polish legal system. The third chapter is devoted to the presentation of the most important instruments of international law, mostly non-binding ones, which introduce guidelines in the personal data protection area. The next, fourth chapter presents the most important laws and areas of regulation related to EU law. The fifth chapter discusses national regulations and the role of the national legislature in the area of privacy protection in cyberspace. The next three chapters refer to selected issues in respect of the most important, in the author's opinion, problems related to the protection of privacy in cyberspace: the sixth chapter pertains to processing in the cloud computing model; the seventh chapter contains an analysis of processing of large data sets (Big Data); in the eighth chapter the possibilities of public authorities related to mass surveillance programs are discussed.

The dissertation ends with a summary in which partial conclusions were collected. On the basis of those conclusions it was determined whether and how international legal norms should be used to create a protective and regulatory framework in the field of the right to privacy in cyberspace.

**Key words:** right to privacy, data protection, cyberspace, international law, transborder data flows, Resolution 2016/679, cloud computing, Big Data, mass surveillance.